SOLUTION BRIEF

How Open Access to Education Creates Security Concerns

Executive Overview

Miami Dade College (MDC), the largest community college in the U.S., was recognized in April 2019 for offering its diverse student body a path to economic prosperity. In the announcement that his institution had won an Aspen Prize, former MDC President Eduardo Padron said, "Open access and academic excellence go hand in hand."[1]

Community colleges make resources—including network resources—broadly available. This is crucial in educating a large and diverse cross-section of the U.S. populace. However, it also creates new IT security risks and increases the complexity of network protection. Especially in an institution facing funding and staffing shortages, a siloed environment may emerge, in which security solutions do not communicate. This reduces visibility into security issues and limits the ability to present a coordinated defense against an attack.

> **"Community colleges … are under constant attack. It only takes one human to click on a link and give up their password for a phishing scheme to succeed."[2]**
>
> *– Henry Glaspie, Associate Vice President, Information Technology, College of Central Florida*

Rapidly Expanding Attack Surface

When it comes to IT security, community colleges face unique challenges. One reason is that students have a number of other significant responsibilities. The vast majority are employed, with 21% of full-time students and 38% of part-time students holding full-time jobs. At the same time, 15% are single parents.[3] Students' external obligations require community colleges to provide broad access to nontraditional learning environments. Students may have difficulty fitting classroom lectures, or even uninterrupted use of a desktop computer, into their hectic schedules.[4] Community colleges are responding by offering mobile, cloud-based solutions, including digital textbooks and research tools. They are also increasingly storing crucial data in major cloud platforms.

In addition, the digital attack surface is expanding in the same way at community colleges as at large universities. Students expect Wi-Fi access for a wide range of devices, including laptops, tablets, smartphones, fitness trackers, smartwatches, computer-enabled shoes, and e-readers.[5] More than half arrive on campus with at least two internet-connected devices, and 22% bring three or four.[6] Each new device, web-connected application, and access point creates an additional security risk that IT teams must address.

Data at Risk

In general, the more facets in a community college's attack surface, the more potential points of entry for hackers. This is a significant concern because a high rate of student turnover[7] and record-retention requirements mean community colleges store a large volume of valuable information.[8] They also store a wide variety of data, which may be subject to different regulations, from financial and personally identifiable information (PII) to health data for students, faculty, and staff, as well as information about students' academic progress.[9]

IT teams must be aware of the different ways in which criminals may infiltrate community college networks. They may pose as college staff or administrators.[10] They also may use social engineering to support these efforts, going as far as applying to the school with the goal of obtaining a legitimate .edu email address to make their schemes more believable.[11]

Gaps in Security

Thwarting such an attack requires a sophisticated IT security environment. Unfortunately, budgets for capital expenditures like security solutions are tight, sometimes nonexistent. State funding of community colleges is unreliable,[12] and 71% of community college presidents say financial issues are a major challenge.[13] For many community colleges, funding issues also reduce the ability to hire skilled security staff. High staff turnover is exacerbated by a skills shortage that makes it hard to fill open positions.[14]

Budgeting constraints can mean that community college networks lack some advanced security features that most businesses deploy, such as sandboxing or security information and event management (SIEM). Staff may lack the expertise or time to effectively monitor a plethora of discrete security solutions. If security products do not integrate tightly, the institution may not have a bird's-eye security perspective. Worse, lack of integration might stymie solutions' ability to respond quickly, in a coordinated way networkwide, when a threat is detected.

Finding the Right Balance

To support their educational mission, community colleges need to maintain networks that are open and welcoming to students, teachers, and staff. At the same time, keeping valuable data secure is critical. As bring-your-own-device (BYOD) and cloud platforms continue to expand schools' digital attack surface, IT staff should look for an integrated network approach with a security fabric that extends protection throughout the network to help secure crucial data and applications.

[1] Ellie Ashford, "Two Florida colleges share Aspen Prize," Community College Daily, April 2, 2019.

[2] Ellie Ashford, "Cyber attacks on the rise at colleges," Community College Daily, September 30, 2018.

[3] "AACC Fast Facts 2019," American Association of Community Colleges, March 2019.

[4] Gina Sipley, "Scaling Mobile Technology for Community College Students: 5 Tips for Entrepreneurs," EdSurge, August 5, 2017.

[5] Bryan Alexander, "When Learning Goes Nomadic," EdSurge, May 2, 2019.

[6] Rhea Kelly, "Survey: Most Students Say Technology Boosts Academic Success," Campus Technology, September 28, 2017.

[7] Aaron R. Warner, "5 Cybersecurity Challenges Unique to Community Colleges—and How to Solve Them," ProCircular, April 20, 2018.

[8] Ellie Ashford, "Cyber attacks on the rise at colleges," Community College Daily, September 30, 2018.

[9] Naveen Goud, "Students are responsible for cyber attacks on Universities and Colleges," Cybersecurity Insiders, accessed August 2019.

[10] Ellie Ashford, "Cyber attacks on the rise at colleges," Community College Daily, September 30, 2018.

[11] Ann McAdams, "Bogus applications plaguing NC college campuses, pose security risk," WECT, June 24, 2019.

[12] Thomas Ridout, "The Top 3 Issues Facing Higher Education CFOs," Forecast5 Analytics, February 6, 2017.

[13] "Challenges and Opportunities Abound for Community Colleges in 2018," McGraw-Hill, May 3, 2018.

[14] Jon Oltsik, "Is the cybersecurity skills shortage getting worse?" CSO, May 10, 2019.

September 4, 2019 10:02 PM

444631-0-0-EN

D:\Fortinet\Work\2019\September\090419\sb-open-access-education